

[Web](#) [Images](#) [Videos](#) [Maps](#) [News](#) [Shopping](#) [Gmail](#) [more ▼](#)
[Scholar Preferences](#) | [Sign in](#)

Google scholar

package restoring cryptographic key

Search

[Advanced Scholar Search](#)

Scholar

Articles and patents

anytime

include citations

[Create email alert](#)Results 1 - 10 of about **43,000**. (0.31 sec)

Apparatus and method for reducing transmission bandwidth and storage requirements in a cryptographic security system

MK Just... - US Patent 6,567,914, 2003 - Google Patents

... The apparatus receives from the requesting recipient, the **key** identification data associated with the requesting recipient and parts of the header data to determine whether at least one of the plurality of **cryptographic key packages** that have been received, corresponds to the ...

Cited by 39 - [Related articles](#) - [All 2 versions](#)

The trustworthy digital camera: Restoring credibility to the photographic image

GL Friedman - Consumer Electronics, IEEE Transactions on, 2002 - [ieeexplore.ieee.org](#)

... 905 THE TRUSTWORTHY DIGITAL CAMERA: **RESTORING CREDIBILITY TO THE PHOTOGRAPHIC IMAGE** Gary L. Friedman Advanced Engineering and ... Digital signatures build upon these public **key cryptographic** techniques and allow you to authenticate the contents of ...

Cited by 257 - [Related articles](#) - [BL Direct](#) - [All 9 versions](#)[\[PDF\] from nasa.gov](#)

Let us remember: cold-boot attacks on encryption keys

JA Halderman, SD Schoen, N Heninger... - ... of the ACM, 2009 - [portal.acm.org](#)

... We present a suite of attacks that exploit DRAM remanence to recover **cryptographic keys** held in memory. They pose a particular threat to laptop users who rely on disk encryption products. An adversary who steals a laptop ...

Cited by 156 - [Related articles](#) - [All 63 versions](#)[\[HTML\] from usenix.org](#)

A public key cryptosystem and a signature scheme based on discrete logarithms

Y ElGamal - Information Theory, IEEE Transactions on, 2002 - [ieeexplore.ieee.org](#)

... Since $p - 1$ is chosen to have at least one large prime factor q , recovering $x \bmod q$ requires an ... that it is better to use $GF(p)$ with $m = 3$ or 4 for implementing a **cryptographic** system ... if the estimates remain the same, then, for the same security level, the size of the public **key** file and ...

Cited by 4192 - [Related articles](#) - [All 11 versions](#)[\[PDF\] from homeip.net](#)

A cryptographic key management scheme for implementing the Data Encryption Standard

WF Ehrsam, SM Matyas, CH Meyer... - IBM Systems J., 2010 - [ieeexplore.ieee.org](#)

... that is, we want to use a session **key** in the form EKMHO(KS) in conjunction with the encipher and decipher operations to respectively create and recover a file. ... However, the advantage of a personal **key** must be weighed against that of **cryptographic** transparency, in which ...

Cited by 91 - [Related articles](#) - [All 5 versions](#)

Method and apparatus for correcting improper encryption and/or for reducing memory storage

L Dillie... - US Patent 6,341,164, 2002 - Google Patents

... US 6,341,164 B1 apparatus 100 may delete ninety nine of the one hundred **cryptographic key packages** (wrapped **keys** K1 and K3-K100 and associated KID data) in the header saving only the wrapped **key**, K2 and KID2, for the one recipient before **restoring** the wrapped **key** ...

Cited by 16 - [Related articles](#) - [All 2 versions](#)

How to share a secret

A Shamir - Communications of the ACM, 1979 - [portal.acm.org](#)

... Such a scheme is called a (k, n) threshold scheme. Efficient threshold schemes can be very helpful in the management of **cryptographic keys**. ... By using a (k, n) threshold scheme with $n = 2k - 1$ we get a very robust **key** management scheme: We can recover the original ...

Cited by 5201 - [Related articles](#) - [Library Search](#) - [All 58 versions](#)[\[PDF\] from cmu.edu](#)

A cryptographic file system for UNIX

M Blaze - Proceedings of the 1st ACM conference on Computer..., 1993 - [portal.acm.org](#)

... These **packages** generally require the preallocation of storage space to a given **key** ... File system services such as backup, **restore**, usage accounting, and archival work normally on ... creates entries in CFS (which appear in/crypt) that associate **cryptographic keys** with directories ...

Cited by 439 - [Related articles](#) - [All 218 versions](#)[\[PDF\] from freedbsd.org](#)

Computer network cryptographic key distribution system

WS Ford... - US Patent 5,481,613, 1996 - Google Patents

... Each legitimate recipient can recover the encryption **key** by decrypting the applicable copy ... possess the encryption and decryption capabilities of a reversible public **key** cryptosystem. There may be a risk of such **cryptographic** capabilities being used for unintended encryption ...

Cited by 89 - [Related articles](#) - [All 5 versions](#)

Computation of cryptographic keys from face biometrics

A Goh... - Communications and Multimedia Security, 2003 - Springer

... $m \times 2^q$ **cryptographic key** in our context. In the simplest linear case, this allows secret recovery via $xf(x) \bmod q$ with $x = x(l, a)$ and $x' = h(l)$. Coordinate pair $(x, f(x))$ constitutes a secret-share, any two of which can be combined to recover a ...

Cited by 36 - [Related articles](#) - [BL Direct](#) - [All 2 versions](#)☐ [Create email alert](#)

Google

Result Page: 1 2 3 4 5 6 7 8 9 10 **Next**

package restoring cryptographic key Search

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

©2011 Google